Network Defender
First Principles

Rick Howard - CSO
Geeks vs Non-Geeks: Reaction to flaky internet connection

Source: Bruno Oliveira
Geeks vs Non-Geeks: Reaction to flaky internet connection

Source: Bruno Oliveira
Geeks vs Non-Geeks: Reaction to flaky internet connection

Source: Bruno Oliveira
Geeks vs Non-Geeks: Reaction to flaky internet connection

Source: Bruno Oliveira
Geeks vs Non-Geeks: Reaction to flaky internet connection

Source: Bruno Oliveira
Geeks vs Non-Geeks: Reaction to flaky internet connection

X-Axis: Time

Source: Bruno Oliveira
Geeks vs Non-Geeks: Reaction to flaky internet connection

Time

Hope

Geek

Non-Geek

Source: Bruno Oliveira
Geeks vs Non-Geeks: Reaction to flaky internet connection

Source: Bruno Oliveira
Geeks vs Non-Geeks: Reaction to flaky internet connection

Source: Bruno Oliveira
Geeks vs Non-Geeks: Reaction to flaky internet connection

Non-Geeks – The Beautiful People

I’ll just wait a bit; maybe it will come back

Source: Bruno Oliveira
Geeks vs Non-Geeks: Reaction to flaky internet connection

Hmmm ... this is taking too long

Non-Geeks – The Beautiful People

Source: Bruno Oliveira
Geeks vs Non-Geeks: Reaction to flaky internet connection

- **Non-Geeks** – The Beautiful People

Source: Bruno Oliveira
Geeks vs Non-Geeks: Reaction to flaky internet connection

Source: Bruno Oliveira
Geeks vs Non-Geeks: Reaction to flaky internet connection

Source: Bruno Oliveira

Non-Geeks – The Beautiful People

Call the ISP

They Are Always so Helpful
Geeks vs Non-Geeks: Reaction to flaky internet connection

Source: Bruno Oliveira

Non-Geeks – The Beautiful People

Call the ISP
Geeks vs Non-Geeks: Reaction to flaky internet connection

Source: Bruno Oliveira
Geeks vs Non-Geeks: Reaction to flaky internet connection

Source: Bruno Oliveira

Geeks – My Peeps
Geeks vs Non-Geeks: Reaction to flaky internet connection

Source: Bruno Oliveira
Geeks vs Non-Geeks: Reaction to flaky internet connection

Source: Bruno Oliveira
Geeks vs Non-Geeks: Reaction to flaky internet connection

Source: Bruno Oliveira
Geeks vs Non-Geeks: Reaction to flaky internet connection

Source: Bruno Oliveira
Geeks vs Non-Geeks: Reaction to flaky internet connection

Source: Bruno Oliveira
Geeks vs Non-Geeks: Reaction to flaky internet connection

- **Geek**
  - Reload
  - Reload
  - Try Another Site
  - Reload
  - Check network settings
  - Switch WiFi On/Off
  - That will fix everything

- **Non-Geek**
  - Reload
  - Reload
  - Reload

Source: Bruno Oliveira
Geeks vs Non-Geeks: Reaction to flaky internet connection

Source: Bruno Oliveira
Geeks vs Non-Geeks: Reaction to flaky internet connection

Source: Bruno Oliveira
Geeks vs Non-Geeks: Reaction to flaky internet connection

Source: Bruno Oliveira

Geeks – My Peeps

Time

Hope

Reload
Reload
Try Another Site
Reload
Check network settings
Switch WiFi On/Off
!
@
#
^!
@&
^!
!
ping
ifconfig
traceroute
dmesg
reboot
iptables

Non-Geek
Geeks vs Non-Geeks: Reaction to flaky internet connection

Source: Bruno Oliveira

Time

Hope

Geeks – My Peeps

- Reload
- Reload
- Try Another Site
- Reload
- Check network settings
- Switch WiFi On/Off
- That will fix everything
- ping
- ifconfig
- traceroute
- dmesg
- reboot
- iptables

Non-Geek

I’ll just wait a bit; maybe it will come back

Source: Bruno Oliveira
Geeks vs Non-Geeks: Reaction to flaky internet connection

Source: Bruno Oliveira

Geeks – My Peeps

Time

Hope

Reload

Reload

Try Another Site

Reload

Check network settings

Switch WiFi On/Off

That will fix everything

!@#$^!@&^!

ping

ifconfig

traceroute

dmesg

reboot

iptables

I’ll just wait a bit; maybe it will come back

Call the ISP

Geek

Non-Geek

Source: Bruno Oliveira
Geeks vs Non-Geeks: Reaction to flaky internet connection

Geeks – My Peeps

Non-Gechs

Hope

Try Another Site

Reload

Check network settings

Switch WiFi On/Off

ping

ifconfig
taxeroute
dmesg
reboot
iptables

That will fix everything

I’ll just wait a bit; maybe it will come back

Call the ISP

They Are Always so Helpful

Source: Bruno Oliveira
Geeks vs Non-Geeks: Reaction to flaky internet connection

Source: Bruno Oliveira

Geeks – My Peeps

Call the ISP

I’ll just wait a bit; maybe it will come back
Geeks vs Non-Geeks: Reaction to flaky internet connection

Source: Bruno Oliveira
Geeks vs Non-Geeks: Reaction to flaky internet connection

Hope vs Time

- Reload
- Try Another Site
- Check network settings
- Switch WiFi On/Off
- ping
- ifconfig
- traceroute
- dmesg
- reboot
- iptables

Geek
- Hmm... this is taking too long
- That will fix everything
- I'll just wait a bit; maybe it will come back

Non-Geek
- Reload
- Reload
- Reload
- Call the ISP

Source: Bruno Oliveira
Geeks vs Non-Geeks: Reaction to flaky internet connection

Source: Bruno Oliveira

I'll just wait a bit; maybe it will come back

Call the ISP

ping
ifconfig
traceroute
dmesg
reboot
iptables

That will fix everything

Load
Try
Another Site

Switch WiFi On/Off

Hmmm … this is taking too long

Geek
Non-GEEK

Time

Hope

On/Off

Source: Bruno Oliveira
Geeks vs Non-Geeks: Reaction to flaky internet connection

Source: Bruno Oliveira
Elon Musk
Elon Musk's Secret Weapon
A Beginner's Guide to First Principles in Business

Elon Musk
What is a First Principle?

Principia Mathematica published in 1913
What is a First Principle?

Principia Mathematica, published in 1913.
What is a First Principle?
Analogy vs First Principle
Analogy vs First Principle

SIMILAR
Analogy vs First Principle
Analogy vs First Principle

LEAP AHEAD

First Principle Thinking
...Challenging the Status Quo

[Image of Elon Musk]
LEAP AHEAD

UNDERSTANDING A QUESTION IS HALF AN ANSWER.

Socrates
LEAP AHEAD

Analogy vs First Principle

First Principle Thinking
...Challenging the Status Quo

Boiled Water
Semantic Tree
Semantic Tree
Semantic Tree

Trunk
Semantic Tree

Limbs
Semantic Tree

Leaves
What is a First Principle?
What is a First Principle?
What is a First Principle?

Fundamental

Self Evident
What is a First Principle?

Fundamental

Self Evident

Experts Agree
What is a First Principle?

Fundamental

Self Evident

Experts Agree

Atomic
What is a First Principle?

- Fundamental
- Self Evident
- Experts Agree
- Atomic
What is a First Principle?

- Fundamental
- Self Evident
- Experts Agree
- Atomic

New

First Principle Thinking
...Challenging the Status Quo
What is a First Principle?

- Fundamental
- Self Evident
- Experts Agree
- Atomic

First Principles
What is a First Principle?

1 + 1 = 2
What is a First Principle?

*Note: Might be useful to know

1 + 1 = 2
Network Defender Problem Space


First Intrusion Detection System
Network Defender Problem Space

1985  First Anti-Virus System
1987  First Intrusion Detection System
1994
2004
2007
2010
2014
Network Defender Problem Space


- First Firewall
- First Anti-Virus System
- First Intrusion Detection System
Network Defender Problem Space

- 1985: First Anti-Virus System
- 1987: First Intrusion Detection System
- 1994: First Firewall
- 2004: First Detection System
- 2007
- 2010
- 2014

Coach’s Playbook

First Innovation 1994 First Firewall
First 1985 1987 First Anti-Virus System
Intrusion Detection System
First 2004 Detection System
Network Defender Problem Space

1985
First Anti-Virus System

1987
First Intrusion Detection System

1994
First Firewall

2010
First Detection System

2014
First Data Loss Protection Systems
Network Defender Problem Space

- 1985: First Anti-Virus System
- 1987: First Intrusion Detection System
- 1994: First Firewall
- 2004: First Data Loss Protection Systems
- 2010: First Detection System

Integration Services

- People
- Process
- Information
- Technology
Network Defender Problem Space

- First Anti-Virus System: 1985
- First Firewall: 1987
- First Intrusion Detection System: 1994
- First Data Loss Protection Systems: 2004
- Complex
- Expensive
- Hard to Manage
Network Defender Problem Space

- First Anti-Virus System (1985)
- First Firewall (1987)
- First Intrusion Detection System (1994)
- First Data Loss Protection Systems

Challenges:
- Complex
- Expensive
- Hard to Manage
Network Defender Problem Space

- 1985: First Anti-Virus System
- 1987: First Intrusion Detection System
- 1994: First Firewall
- 2004: First Data Loss Protection Systems
- 2007: First Detection System
- 2010
- 2014
Network Defender Problem Space

- 1985: First Anti-Virus System
- 1987: First Intrusion Detection System
- 1994: First Firewall
- 2004: First Data Loss Protection Systems
- 2007: First Detection System
- 2014: Leap Ahead
Network Defender Problem Space

- First Anti-Virus System: 1985
- First Firewall: 1987
- First Intrusion Detection System: 1994
- First Detection System: 2004
- First Data Loss Protection Systems: 2007
Prefatory First Principle Statements

Whitehead

Russell

Principia Mathematica
Prefatory First Principle Statements

Network Defenders
Prefatory First Principle Statements

Network Defenders

<table>
<thead>
<tr>
<th>Cyber Espionage</th>
<th>Cyber Crime</th>
<th>Cyber Hacktivism</th>
<th>Cyber Warfare</th>
<th>Cyber Mischief</th>
<th>Cyber Terrorism</th>
</tr>
</thead>
</table>

Lego's Playbook
Prefatory First Principle Statements

<table>
<thead>
<tr>
<th>CYBER ESPIONAGE</th>
<th>![Spy icon]</th>
</tr>
</thead>
<tbody>
<tr>
<td>CYBER CRIME</td>
<td>![Lock icon]</td>
</tr>
<tr>
<td>CYBER HACKTIVISM</td>
<td>![Computer icon]</td>
</tr>
<tr>
<td>CYBER WARFARE</td>
<td>![Mounted icon]</td>
</tr>
<tr>
<td>CYBER MISCHIEF</td>
<td>![Spider icon]</td>
</tr>
<tr>
<td>CYBER TERRORISM</td>
<td>![Fire icon]</td>
</tr>
</tbody>
</table>

---

Network Defenders

![Superhero image]
Prefatory First Principle Statements
Prefatory First Principle Statements
Prefatory First Principle Statements
Prefatory First Principle Statements

Coach’s Playbook

Gettysburg Campaign

Source: "THOUGHTS, ESSAYS, AND MUSINGS ON THE CIVIL WAR," by Bob.
http://books.google.com/books?id=2009101-gettysburg_campaign part 1/2.html

Victim
Wow! That’s a lot!

Prefatory First Principle Statements
Prefatory First Principle Statements

Risk Matrix
X-Axis: Likelihood
Risk Matrix
Prefatory First Principle Statements

Risk Matrix

Y-Axis: Impact
What is a Network Defender First Principle?
What is a Network Defender First Principle?
What is a Network Defender First Principle?
What is a Network Defender First Principle?
What is a Network Defender First Principle?
What is a Network Defender First Principle?
What is a Network Defender First Principle?
What is a Network Defender First Principle?
What is a Network Defender First Principle?

What is it?

What should it be?
What is it?

What should it be?

What do we agree that it should be?
What is a Network Defender First Principle?

“We must identify the trunk and the big branches first so that when we discover the leaves later, we will have something to hang them on.”
Network Defender Semantic Tree
Network Defender Semantic Tree

1 Trunk
5 Limbs
Network Defender Semantic Tree

Leaves
Network Defender Semantic Tree: *The Trunk*
Network Defender Semantic Tree: The Trunk
Network Defender Semantic Tree: The Trunk
Network Defender Semantic Tree: *The Trunk*

*Trunk*  Prevent High Risk Material Impact
Network Defender Semantic Tree: The Trunk

Trunk
Network Defender Semantic Tree: The Trunk
Network Defender Semantic Tree: The Trunk
Network Defender Semantic Tree: The Trunk
Network Defender Semantic Tree: The Trunk
Network Defender Semantic Tree: **The Trunk**
Network Defender Semantic Tree: The Trunk
Network Defender Semantic Tree: The Trunk

Trunk

High Probability

Network Defenders

Gettysburg Campaign

Source: "THOUGHTS, ESSAYS, AND REMINISCENCES ON THE CIVIL WAR," by Bii.

paloalto

Network Defender Semantic Tree: The Trunk

Trunk

High Probability

Network Defenders

Gettysburg Campaign

Source: "THOUGHTS, ESSAYS, AND REMINISCENCES ON THE CIVIL WAR," by Bii.

paloalto
Network Defender Semantic Tree: The Trunk

High Damage

Trunk

High Probability

Gettysburg Campaign

Source: "THOUGHTS, ESSAYS, AND VIEWS ON THE CIVIL WAR," by B.F.C.
Network Defender Semantic Tree: The Trunk

Prevent High Risk Material Impact

Prevent High Risk Material Impact
The First Limb
Network Defender Semantic Tree: First Limb

Limb

Establish a Robust Threat Prevention program
Network Defender Semantic Tree: First Limb

Network Defenders
Network Defender Semantic Tree: First Limb
Network Defender Semantic Tree: First Limb
Network Defender Semantic Tree: First Limb

Network Defenders

DON'T WASTE NATURAL RESOURCES

NEW
Network Defender Semantic Tree: First Limb

Network Defenders

NEW

DON'T WASTE NATURAL RESOURCES

Coach's Playbook
Network Defender Semantic Tree: First Limb
Network Defender Semantic Tree: First Limb
Network Defender Semantic Tree: First Limb

Victim
Network Defender Semantic Tree: First Limb

IOC Set
Indicators of Compromise

- Motive
- Attack Objective
- Delivery
- Exploitation
- Command and Control
- Lateral Movement
- Actions on the Objective
Indicators of Compromise are forensic artifacts that describe an adversary’s methodology; digital clues left behind by the adversary group as it works its way through the phases of the attack lifecycle.
Indicators of Compromise are forensic artifacts that describe an adversary’s methodology; digital clues left behind by the adversary group as it works its way through the phases of the attack lifecycle.
Indicators of Compromise are forensic artifacts that describe an adversary’s methodology; digital clues left behind by the adversary group as it works its way through the phases of the attack lifecycle.
The attack life cycle is a phased model that describes the tasks an adversary group must accomplish in order to complete their mission.
The **attack life cycle** is a phased model that describes the tasks an adversary group must accomplish in order to complete their mission.
The **attack life cycle** is a phased model that describes the tasks an adversary group must accomplish in order to complete their mission.
The **attack life cycle** is a phased model that describes the tasks an adversary group must accomplish in order to complete their mission.
The attack life cycle is a phased model that describes the tasks an adversary group must accomplish in order to complete their mission.
The attack life cycle is a phased model that describes the tasks an adversary group must accomplish in order to complete their mission.
The **attack life cycle** is a phased model that describes the tasks an adversary group must accomplish in order to complete their mission.
Network Defender Semantic Tree: First Limb
Network Defender Semantic Tree: First Limb
Network Defender Semantic Tree: First Limb
Network Defender Semantic Tree: First Limb

IOC Set
- Indicators of Compromise
  - Motive
  - Attack Objective
  - Delivery
  - Exploitation
  - Command and Control
  - Lateral Movement
  - Actions on the Objective
Network Defender Semantic Tree: First Limb
Network Defender Semantic Tree: First Limb

Gettysburg Campaign

Coach's Playbook

IOC Set
- Motive
- Attack Objective
- Delivery
- Exploitation
- Command and Control
- Lateral Movement
- Actions on the Objective
Network Defender Semantic Tree: First Limb
Network Defender Semantic Tree: First Limb
Network Defender Semantic Tree: First Limb
Threat Prevention is the act of turning known indicators of compromise into one or more deployed prevention controls.
Threat Prevention is the act of turning known indicators of compromise into one or more deployed prevention controls.
Network Defender Semantic Tree: First Limb

Gather Intelligence
Plan the Attack

Leverage Exploit
Silent Infection

Exe Mal
Malicious File Executed

Preventive Controls

Steal Data
Malware Communicates with Attacker
Data Theft, Sabotage, Destruction

Reactive Controls
Network Defender Semantic Tree: **First Limb**

**Preventive Controls**
- Plan the Attack
- Silent Infection
- Malicious File Executed
- Malware Communicates with Attacker

**Reactive Controls**
- Data Theft, Sabotage, Destruction

**Gettysburg Campaign**

**Prevention Control**
Network Defender Semantic Tree: First Limb

**Gather Intelligence**
- Plan the Attack

**Leverage Exploit**
- Silent Infection

**Execute Malware**
- Malicious File Executed
- Malware Communicates with Attacker

**Steal Data**
- Data Theft, Sabotage, Destruction

**Preventive Controls**
- PRECISION

**Reactive Controls**
- Prevention Control
Network Defender Semantic Tree: First Limb

**Preventive Controls**
- Plan the Attack
- Silent Infection
- Malicious File Executed
- Malware Communicates with Attacker

**Reactive Controls**
- Data Theft, Sabotage, Destruction
Network Defender Semantic Tree: **First Limb**

**Preventive Controls**
- Plan the Attack
- Silent Infection
- Malicious File Executed

**Reactive Controls**
- Malware Communicates with Attacker
- Data Theft, Sabotage, Destruction

**Control Channel**
- Malware

**Execute Malware**
- Attacker

**Let Down Exploit**
- Hacker
Network Defender Semantic Tree: First Limb

99% Guarantee

Preventive Controls

Plan the Attack
Silent Infection
Malicious File Executed
Malware Communicates with Attacker
Data Theft, Sabotage, Destruction

Reactive Controls

Prevention Control

Gather Intelligence
Leverage Exploit
Execute Malware
Control Channel
Steal Data

99% GUARANTEE
Network Defender Semantic Tree: First Limb

99% GUARANTEE
Network Defender Semantic Tree: First Limb

- **Gather Intelligence**: Plan the Attack
- **Leverage Exploit**: Silent Infection
- **Execute Malware**: Malicious File Executed
- **Control Channel**: Malware Communicates with Attacker
- **Steal**: Data Theft, Sabotage, Destruction

**Preventive Controls**

**Reactive Controls**
Network Defender Semantic Tree: *First Limb*

1st Limb

Establish a Robust Threat Prevention program
Establish a Robust Threat Detection Program

Network Defender Semantic Tree: 2d Limb

Limb
Network Defender Semantic Tree: 2d Limb

NOT ENOUGH
Network Defender Semantic Tree: 2d Limb
Network Defender Semantic Tree: 2d Limb
Network Defender Semantic Tree: 2d Limb
Network Defender Semantic Tree: 2d Limb
Network Defender Semantic Tree: 2d Limb

Network Defenders

Threat Prevention
Network Defender Semantic Tree: 2d Limb

Network Defenders

Threat Prevention

Prevent High Risk Material Impact

EPIC FAIL
Network Defender Semantic Tree: 2d Limb

#1

Prevent High Risk Material Impact

EPIC FAIL
Network Defender Semantic Tree: 2d Limb

#1

Coach’s Playbook

Prevent High Risk Material Impact

EPIC FAIL
Network Defender Semantic Tree: 2d Limb
Network Defender Semantic Tree: 2d Limb

#2

Prevent High Risk Material Impact

EPIC FAIL
Network Defender Semantic Tree: 2d Limb

#2

Threat Prevention

Prevent High Risk Material Impact

EPIC FAIL
Network Defender Semantic Tree: 2d Limb

Threat Detection
Network Defender Semantic Tree: 2d Limb

Threat Detection

Hunting
Network Defender Semantic Tree: 2d Limb

Threat Detection

Hunting

IOC Set
Indicators of Compromise

Motive
Attack Objective
Delivery
Exploitation
Command and Control

SOMETHING INCREDIBLE is waiting to be KNOWN
Network Defender Semantic Tree: 2d Limb
Network Defender Semantic Tree: 2d Limb
Network Defender Semantic Tree: 2d Limb
Network Defender Semantic Tree: 2d Limb

Threat Detection

Hunting

IOC Set
Indicators of Compromise

Motive
Attack Objective
Delivery
Exploitation
Command and Control

SOMEBODY
SOMETHING
INCREDIBLE
is waiting to be
KNOWN

act now
Establish a Robust Threat Detection Program
The Third Limb
Network Defender Semantic Tree: 3rd Limb

3rd Limb

Establish a Robust Threat Eradication Program
Network Defender Semantic Tree: 3rd Limb

Threat Detection
Network Defender Semantic Tree: 3rd Limb

Threat Detection

SOMETHING INCREDIBLE is waiting to be KNOWN

somewhere
Network Defender Semantic Tree: 3rd Limb

Threat Detection

SOMETHING INCREDIBLE is waiting to be KNOWN

Network Defenders
Network Defender Semantic Tree: 3rd Limb

Threat Detection

SOMETHING INCREDIBLE is waiting to be KNOWN

Network Defenders
Threat eradication is the act of **minimizing** the effectiveness of newly discovered adversary campaign activity by **blocking** future activity through the Threat Prevention program, analyzing the purpose of this new campaign, and installing additional countermeasures that will likely thwart the accomplishment of the campaign objectives.
Threat eradication is the act of minimizing the effectiveness of newly discovered adversary campaign activity by blocking future activity through the Threat Prevention program, analyzing the purpose of this new campaign, and installing additional countermeasures that will likely thwart the accomplishment of the campaign objectives.
Network Defender Semantic Tree: 3rd Limb
Network Defender Semantic Tree: 3rd Limb

#1

IOC Set
Indicators of Compromise
- Motive
- Attack Objective
- Delivery
- Exploitation
- Command and Control
- Lateral Movement
- Actions on the Object

SOMEBODY, SOMETHING INCREDIBLE is waiting to be KNOWN

Prevention Control

Network Defenders
Network Defender Semantic Tree: 3rd Limb

#2

Motivations
- CYBER ESPIONAGE
- CYBER CRIME
- CYBER HACKTIVISM
- CYBER WARFARE
- CYBER MISCHIEF
- CYBER TERRORISM

Objectives
Network Defender Semantic Tree: 3rd Limb

#2

Motivations
- Cyber Espionage
- Cyber Crime
- Cyber Hacktivism
- Cyber Warfare
- Cyber Mischief
- Cyber Terrorism

Objectives

Network Defenders
Network Defender Semantic Tree: 3rd Limb

Establish a Robust Threat Eradication Program
The Fourth Limb
Create the Network Defender’s Trinity.
Network Defender Semantic Tree: 4th Limb

- Threat Detection
- Threat Prevention
- Threat Eradication
Network Defender Semantic Tree: 4th Limb

- Threat Detection
- Threat Prevention
- Threat Eradication
Inextricably linked
Network Defender Semantic Tree: 4th Limb

Inextricably linked
Network Defender Semantic Tree: 4th Limb

Inextricably linked

Network Defender’s Trinity

Threat Prevention

Threat Detection

Threat Eradication

irreducible complexity
Network Defender Semantic Tree: 4th Limb

Network Defenders

Trinity

Network Defender’s Trinity

Threat Prevention

Threat Detection

Threat Eradication
Create the Network Defender’s Trinity.
Embrace cybersecurity intelligence collection and ubiquitous sharing
Network Defender Semantic Tree: 5th Limb
Network Defender Semantic Tree: 5th Limb
Network Defender Semantic Tree: 5th Limb

Collected
Network Defender Semantic Tree: 5th Limb

Collected
Sorted
Network Defender Semantic Tree: 5th Limb

Collected
Sorted
Evaluated
Network Defender Semantic Tree: 5th Limb

Collected
Sorted
Evaluated
Prioritized
Intelligence collection is the act of gathering Indicators of Compromise from network and endpoint systems throughout the enterprise and discovering any supplemental information from internal and external sources that can add context about what the adversary group is about.
Intelligence collection is the act of gathering **Indicators of Compromise** from **network and endpoint** systems throughout the enterprise and discovering any supplemental information from internal and external sources that can **add context** about what the adversary group is about.
Network Defender Semantic Tree: 5th Limb

Network Defenders
Network Defender Semantic Tree: 5th Limb
Network Defender Semantic Tree: 5th Limb

Maximize
Network Defender Semantic Tree: 5th Limb
Network Defender Semantic Tree: 5th Limb

Network Defenders

IOC Set

Indicators of Compromise

Motive
Attack Objective
Delivery
Exploitation
Command and Control
Lateral Movement
Achieving the Goal

Threat Prevention

Threat Detection

Threat Eradication
Network Defender Semantic Tree: 5th Limb

Network Defenders

IOC Set
Indicators of Compromise
- Motive
- Attack Objective
- Delivery
- Exploitation
- Command and Control
- Lateral Movement
- Achieve the Objective

WHERE SOMEWHERE INCREASINGLY KNOWN

Somewhere
Indicators of Compromise

Network Defender’s Trinity

Threat Prevention

Threat Detection

Threat Eradication

NEW

Palo Alto Networks
Network Defender Semantic Tree: 5th Limb

Hard Work

intelligence
Network Defender Semantic Tree: 5th Limb

- Hard Work
- Intelligence
- Inefficiency
Network Defender Semantic Tree: 5th Limb
Network Defender Semantic Tree: 5th Limb

Benefits

#1

All
Network Defender Semantic Tree: 5th Limb

Benefits

#2
Embrace cybersecurity intelligence collection and ubiquitous sharing
The Cyber Threat Alliance
Founding CEOs

Mark McLaughlin  Michael Brown  Ken Xie  Chris Young
Founding Members:

Purpose: The Cyber Threat Alliance is a group of cyber security practitioners that have chosen to share threat information with each other for the purpose of improving defenses against advanced cyber adversaries across member organizations and their customers.
Working Committee
2 Initial Issues

Build Trust

Build Infrastructure
New Contributing Members:

Membership: Open to any organization that can share a minimum volume of threat intelligence designed by the Alliance.
New Contributing Members:

Membership: Open to any organization that can share a minimum volume of threat intelligence designed by the Alliance.

White House Summit on Cybersecurity and Consumer Protection held at Stanford University
Two Unique Organizing Principles:

• **Must Contribute.**

• **Whatever is shared goes directly into the product line.**

Result: **Automatic Prevention Controls.**
Founding CEOs

Mark McLaughlin
Michael Brown
Ken Xie
Chris Young
Founding CEOs

Mark McLaughlin
Michael Brown
Ken Xie
Chris Young
Cyber Threat Alliance

CryptoWall version 3
RANSOMWARE
Security vendors join together and reveal lucrative ransomware attacks affecting hundreds of thousands of users:

⚠️ $325M in estimated damages across the globe

× 839 command and control URLs
× 5 second-tier IP addresses used for command and control

🔍 49 campaign code identifiers

⚠️ 406,887 attempted infections of CryptoWall version 3

bio 4,046 malware samples
RANSOMWARE
Security vendors join together and reveal lucrative ransomware attacks affecting hundreds of thousands of users:

- $325M in estimated damages across the globe
- 839 command and control URLs
- 5 second-tier IP addresses used for command and control
- 49 campaign code identifiers
- 406,887 attempted infections of CryptoWall version 3
- 4,046 malware samples
CryptoWall version 3

RANSOMWARE
Security vendors join together and reveal lucrative ransomware attacks affecting hundreds of thousands of users:

- $325M in estimated damages across the globe
- 839 command and control URLs
- 5 second-tier IP addresses used for command and control
- 49 campaign code identifiers
- 406,887 attempted infections of CryptoWall version 3
- 4,046 malware samples
CryptoWall version 3

RANSOMWARE
Security vendors join together and reveal lucrative ransomware attacks affecting hundreds of thousands of users:

$325M in estimated damages across the globe

839 command and control URLs

5 second-tier IP addresses used for command and control

49 campaign code identifiers

406,887 attempted infections of CryptoWall version 3

4,046 malware samples
CryptoWall version 3

RANSOMWARE
Security vendors join together and reveal lucrative ransomware attacks affecting hundreds of thousands of users:

- $325M in estimated damages across the globe
- 839 command and control URLs
- 5 second-tier IP addresses used for command and control
- 49 campaign code identifiers
- 406,887 attempted infections of CryptoWall version 3
- 4,046 malware samples
Cyber Threat Alliance Cryptowall Dashboard

CryptoWall Version 3

Ransomware

Security vendors join together and reveal lucrative ransomware attacks affecting hundreds of thousands of users:

- $325M in estimated damages across the globe
- 839 command and control URLs
- 5 second-tier IP addresses used for command and control
- 49 campaign code identifiers
- 406,887 attempted infections of CryptoWall version 3
- 4,046 malware samples
CrypToWall version 3

RANSOMWARE
Security vendors join together and reveal lucrative ransomware attacks affecting hundreds of thousands of users:

-$325M in estimated damages across the globe
-839 command and control URLs
-5 second-tier IP addresses used for command and control
-49 campaign code identifiers
-406,887 attempted infections of CryptoWall version 3
-4,046 malware samples
CryptoWall version 3

RANSOMWARE

Security vendors join together and reveal lucrative ransomware attacks affecting hundreds of thousands of users:

- $325M in estimated damages across the globe
- 839 command and control URLs
- 8 second-tier IP addresses used for command and control
- 49 campaign code identifiers
- 406,887 attempted infections of CryptoWall version 3
- 4,046 malware samples
The only smart thing for the network defender to do is to share everything; crowd source threat intelligence so that only the advanced adversary can keep up.
25 Years of Incremental Improvement

- 1985: First Anti-Virus System
- 1987: First Intrusion Detection System
- 1994: First Firewall
- 2004: First Data Loss Protection Systems
- 2007: First Detection System
- 2010
- 2014
Rethink the Network Defender Problem Space

LEAP AHEAD

First Principle Thinking
...Challenging the Status Quo

Boiled Water
Rethink the Network Defender Problem Space

Whitehead

Russell

Elon Musk
Fundamental
Self Evident
Experts Agree
Atomic

Rethink the Network Defender Problem Space
Semantic Tree

Limbs

Trunk
Network Defender First Principles

Prevent High Risk Material Impact
Establish a Robust Threat Prevention program
Network Defender First Principles

2nd Limb

Establish a Robust Threat Detection Program
Network Defender First Principles

3rd Limb

Establish a Robust Threat Eradication Program
The Network Defender’s trinity is inextricably linked, atomic, and irreducible
Embrace cybersecurity intelligence collection and ubiquitous sharing
Call to Action

First Principle White Paper:

Rick Howard: CSO Palo Alto Networks
Email: rhoward@paloaltonetworks.com
Twitter: @raceBannon99

http://cyberthreatalliance.org/

https://paloaltonetworks.com/threat-research.html

https://paloaltonetworks.com/threat-research/cybercanon.html